UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,773	03/09/2004	Mark Ammar Rayes	50325-0865	4164

29989 7590 04/15/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER	
SHAIFER HARRIMAN, DANT B	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
04/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/797,773	RAYES ET AL.	
	Examiner	Art Unit	
	DANT B. SHAIFER HARRIMAN	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 14 & 16 - 20 & 24 - 26 & 28 - 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 - 14 & 16 - 20 & 24 - 26 & 28 - 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to applicants response filed on 01/31/2008.

- Claims 1, 3, 4 - 6, 9, 10, 12, 14, 16 - 18, 20, 24, 25, 26, 28, 29 – 31 are amended in the instant pending application.
- Claims 15, 21 – 23, 27 cancelled in the instant pending application.
- Claims 2, 8, 11, 13 are original in the instant pending application.
- Claim 7 is previously presented in the instant pending application.
- Claims 32 – 42 are new claims presented in the instant pending application.

Response to Arguments

- Applicants arguments with respect to claims 1 – 42 have been considered but are moot in view of the new grounds of rejection, please see the office action below.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim(s) 1- 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomsen (US Patent NO. 7194004 B1) in view of Renda et al. (US Patent NO. 7127524 B1)

Thomsen discloses:

1. A method, comprising the computer-implemented steps of:

- in response to the security event, causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users (Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that un-trusted

and trusted IP addresses are different); and

- configuring one or more security restrictions with respect to the selected new network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56).

3. A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the step of causing the network device to acquire the new network address comprises resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 - 64).

4. A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the step of causing the network device to acquire the new network address comprises issuing a DHCP FORCE_RENEW message to the network device(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 11, lines 56 - 60).

5. A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the step of causing the network device to acquire the new network address comprises prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64).

6. A method as recited in Claim 1, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the step of causing the network device to acquire the new network address comprises waiting for expiration of a lease for a current network address of the network device (Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 11, lines 56 - 60).

7. A method as recited in Claim 1, wherein

- the step of causing the network device to acquire the new network address comprises the step of providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

8. A method as recited in Claim 7, further comprising

- the step of publishing information describing characteristics of the special IP subnet to network service providers(Col. 9, lines 36 - 38).

12. A method as recited in Claim 1, further comprising the steps of determining

- whether a malicious act caused the security event, and if not, removing the user from the second specified pool(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

13. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, wherein a legal user action in the network is not determined to be a malicious act if the user is associated with a trusted customer of a network service provider(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

14. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- receiving information identifying a security event in the network(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- configuring one or more security restrictions with respect to the selected new network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56);

- determining whether a malicious act caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

if a malicious act caused the security event, then providing information about the security event or malicious act to a security

decision controller(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

if a malicious act did not cause the security event, then removing the user from the elevated risk group(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails).

16. A method as recited in Claim 14, wherein causing the network device to acquire the new network address comprises the steps of:

- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

  and

performing any one of the steps of:

(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP();

(b) issuing a DHCP FORCE_RENEW message to the network device();

(c) prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64); or

(d) waiting for expiration of a lease for the first network address of the network device().

18. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of (Col. 12, lines 43 - 59):

- in a security controller that is coupled, through a network, to a network device having first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- in response to the security event, causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col.

5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- and configuring one or more security restrictions with respect to the new network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56).

19. An apparatus, comprising:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- means for, in response to the security event, causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- and means for configuring one or more security restrictions with respect to the new network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56).

20. An apparatus, comprising:

- a network interface that is coupled to a data network for receiving one or more packet flows therefrom(Col. 5, lines 9 – 17, Col. 11, lines 23 – 34, the firewall or gateway is considered as a network interface that is coupled to the data network);

- a processor(Col. 12, lines 60 - 64);

- one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of(Col. 12, lines 43 - 49):

- in a security controller that is coupled, through the data network, to a network device having a first network address assigned from a first subset of addresses within a first

specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- in response to the security event, causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- and configuring one or more security restrictions with respect to the new network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56).

24. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- receiving information identifying a security event in the network(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 –

63, Col. 12, lines 4 – 9);

- configuring one or more security restrictions with respect to the new network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56);

- determining whether a malicious act caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- if a malicious act did not cause the security event, then removing the user from the elevated risk group(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

25. An apparatus comprising

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- means for receiving information identifying a security event in the network(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9, the examiner notes that the security event is interpreted as if the authentication of the device fails);

- means for correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- means for, in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- means for configuring one or more security restrictions with respect to the new network address(Col. 11, lines 23 – 34, Col. 11, lines 51 – 56);

- means for determining whether a malicious act caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- means for, if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- means for, if a malicious act did not cause the security event, then removing the user from the elevated risk group(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

26. An apparatus, comprising:

- a network interface that is coupled to a data network for receiving one or more packet flows therefrom(Col. 5, lines 9 – 17, Col. 11, lines 23 – 34, the firewall or gateway is considered as a network interface that is coupled to the data network to allow for packet flow to the data network);

- a processor(Col. 12, lines 60 - 64); and

- one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out(Col. 12, lines 43 - 49):

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9):

- receiving information identifying a security event in the network(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

wherein

- the second subset of addresses is different from the first subset of addresses(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- configuring one or more security restrictions with respect to the new network address(Col. 11, lines 23 – 34, Col. 11,

lines 51 – 56);

- determining whether a malicious act caused the security event(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

- if a malicious act did not cause the security event, then removing the user from the elevated risk group(Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9).

28. The apparatus of claim 26, wherein the instructions which when executed cause the network device to acquire a new network address comprise further instructions which when executed cause:

- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9); and

performing any one of the steps of:

(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP();

(b) issuing a DHCP FORCE_RENEW message to the network device();

(c) prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64); or

(d) waiting for expiration of a lease for a the first network address of the network device().

30. The apparatus of claim 20, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the instructions which when executed cause the network device to acquire a new network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 - 64).

31. The apparatus of claim 20, wherein

- instructions which when executed cause the network device to acquire a new network address comprise instructions which when executed cause providing the network device

with an IP address that is selected from a plurality of IP addresses within a special IP subnet(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 12, lines 43 - 49).

32. The apparatus of claim 20, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the instructions which when executed cause the network device to acquire a new network address comprise instructions which when executed cause issuing a DHCP FORCE_RENEW message to the network device(Col. 11, lines 56 - 60).

33. The computer-readable storage medium of claim 18, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the instructions which, when executed, cause the network device to acquire the new network address comprise instructions which when executed cause resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP (Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 12, lines 43 - 49).

34. The computer-readable storage medium of claim 18, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the

instructions which when executed cause the network device to acquire the new network address comprise instructions which when executed cause issuing a DHCP FORCE_RENEW message to the network device (Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 11, lines 56 - 60).

35. The computer-readable storage medium of claim 18, wherein

- instructions which when executed cause the network device to acquire a new network address comprise instructions which when executed cause providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 12, lines 43 - 49).

36. The apparatus of claim 19, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the means for causing the network device to acquire the new network address comprise means for resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64).

37. The apparatus of claim 19, wherein

- the network device uses dynamic host control protocol (DHCP) to obtain the new network address, and wherein the means for causing the network device to acquire the new

network address comprise means for issuing a DHCP FORCE_RENEW message to the network device(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 11, lines 56 - 60).

38. The apparatus of claim 19, wherein

- the means for causing the network device to acquire a new network address comprise means for providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64).

39. The computer-readable storage medium of claim 24, wherein the instructions which when executed cause the network device to acquire a new network address comprise further instructions which when executed cause (Col. 12, lines 43 - 59):

- re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9);

and performing any one of the steps of:

(a) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP();

(b) issuing a DHCP FORCE_RENEW message to the network device();

(c) prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64); or

(d) waiting for expiration of a lease for the first network address of the network device().

41. The apparatus of claim 25, wherein the means for causing the network device to acquire a new network address further comprise:

- means for re-configuring a dynamic host control protocol (DHCP) server to require said server to issue any new network address to the network device only from a specified group of network addresses that is reserved for users associated with elevated user risk(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64 and Col. 5, lines 54 – 65, Col. 11, lines 62 – 63, Col. 12, lines 4 – 9); and

means for performing any one of the steps of:

(e) resetting a port that is coupled to the network device to trigger the network device to request a new network address using DHCP();

(f) issuing a DHCP FORCE_RENEW message to the network device();

(g) prompting the network device to request a new network address using DHCP(Col. 8, lines 12 – 14, Col. 10, lines 62 – 64); or

(h) waiting for expiration of a lease for the first network address of the network device().

Thomsen does not explicitly disclose:

1. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:

- determining a user identifier associated with the network device that has caused a security event in the network;

2. A method as recited in Claim 1, further comprising the steps of:

- receiving information identifying the security event in the network;

- correlating the security event information with network user information to result in determining the user identifier associated with the network device.

9. A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address.

10. A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the new network address.

11. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller.

17. A method as recited in Claim 14, wherein the step of configuring one or more security restrictions comprises the steps of:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address;

- and modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the new network address.

18. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

- determining a user identifier associated with the network device that has caused a security event in the network();

19. An apparatus, comprising:

- means for determining a user identifier associated with the network device that has caused a security event in the network();

20. An apparatus, comprising:

- determining a user identifier associated with the network device that has caused a security event in the network();

29. The apparatus of claim 26, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address; and

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the new network address.

40. The computer-readable storage medium of claim 24, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address; and

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the new network address.

42. The apparatus of claim 25, wherein the means for configuring one or more security restrictions comprise:

- means for modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address; and

- means for modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the new network address.

However, Renda discloses:

1. A method, comprising the computer-implemented steps of:

- in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users (Col. 8, lines 48 – 58, Col. 24, lines 13 - 23, Col. 25, lines 3 - 16, Col. 27, Col. 7, lines 45 - 62, lines 52 - 57, the examiner notes that the security controller is considered the master access controller or access controller):

- determining a user identifier associated with the network device that has caused a security event in the network(Col. 9, lines 45 - 55, Col. 23, lines 31 - 33, Col. 24, lines 3 - 9);

2. A method as recited in Claim 1, further comprising the steps of:

- receiving information identifying the security event in the network(Col. 7, lines 63 – 67, col. 8, lines 1 - 14);

- correlating the security event information with network user information to result in determining the user identifier associated with the network device(Col. 7, lines 63 – 67, col. 8, lines 1 - 14).

9. A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address(Col. 10, lines 54 - 64).

10. A method as recited in Claim 1, wherein

- the step of configuring security restrictions comprises the steps of modifying a media access control (MAC) ACL associated with a port that is coupled to the network device to permit entry of traffic only for a MAC address that is bound to the new network address(Col. 10, lines 44 - 48).

11. A method as recited in Claim 1, further comprising

- the steps of determining whether a malicious act caused the security event, and if so, providing information about the security event or malicious act to a security decision controller(Col. 7, lines 63 - 67, Col. 8, lines 1 - 14).

17. A method as recited in Claim 14, wherein the step of configuring one or more security restrictions comprises the steps of:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address(Col. 10, lines 54 - 64);

- and modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the new network address(Col. 10, lines 44 - 48).

18. A computer-readable storage medium carrying one or more sequences of instructions, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of (Col. 6, lines 4 – 18, Col. 6, lines 34 – 48):

- determining a user identifier associated with the network device that has caused a security event in the network(Col.

9, lines 45 - 55, Col. 23, lines 31 - 33, Col. 24, lines 3 - 9);

19. An apparatus, comprising:

- means for determining a user identifier associated with the network device that has caused a security event in the network(Col. 9, lines 45 - 55, Col. 23, lines 31 - 33, Col. 24, lines 3 - 9);

20. An apparatus, comprising:

- determining a user identifier associated with the network device that has caused a security event in the network(Col. 9, lines 45 - 55, Col. 23, lines 31 - 33, Col. 24, lines 3 - 9);

29. The apparatus of claim 26, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause:

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address (Col. 10, lines 54 - 64); and

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address

that is bound to the new network address (Col. 10, lines 44 - 48).

40. The computer-readable storage medium of claim 24, wherein the instructions which when executed cause configuring one or more security restrictions comprise instructions which when executed cause (Col. 6, lines 4 – 18, Col. 6, lines 34 – 48):

- modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address (Col. 10, lines 54 - 64); and

- modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the new network address (Col. 10, lines 44 - 48).

42. The apparatus of claim 25, wherein the means for configuring one or more security restrictions comprise:

- means for modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the new network address (Col. 10, lines 54 - 64); and

- means for modifying a media access control (MAC) ACL associated with the port to permit entry of traffic only for a MAC address that is bound to the new network address (Col. 10, lines 44 - 48).

Thomsen and Renda are analogous art because they are from the "same field of endeavor," which is the field of secure accessing of a network.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Thomsen and Renda before him or her, to modify an electronic device acquiring an internet protocol address from a pool of internet protocol addresses of known malicious user of the internet of Thomsen to include a security controller to judge whether or not the user should obtain an address from pool of internet protocol addresses that are not associated with malicious user or the user should obtain an internet address from a pool of internet protocol addresses that are associated with malicious from of Renda.

The suggestion/motivation for doing so would have been to see

KSR v. **Teleflex**, 127 S.Ct. 1727, 1740, 82 USPQ2d 1385, 1396

(2007)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DANT B. SHAIFER HARRIMAN whose telephone number is (571)272-7910. The examiner can normally be reached on Monday - Thursday: 8:00am - 5:30pm Alt.Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Dant B Shaifer - Harriman /
Examiner, Art Unit 2134

4/02/2008

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2134